

Chapter 2

C001 USER ORIENTATION

Para	Title	Page
2.1.	AFEMS (C001) User Security Access Policy and Procedures	2-1
2.2.	User LOGON to AFEMS (C001).....	2-2
2.3.	AFEMS Main Menu.....	2-3
2.4.	Help.....	2-4

NOTE: Throughout this chapter the Air Force Equipment Management System (AFEMS) may be referred to only as C001 and Department of Defense (DoD) personnel are referred to only as users.

2.1. AFEMS (C001) User Security Access Policy and Procedures.

2.1.1. General. This section establishes policy and procedures, and assigns responsibilities to assure that the appropriate requirements of AFSSI 5102, *The Computer Security (COMPUSEC) Program*, are satisfied for user access of AFEMS (C001).

2.1.2. References.

2.1.2.1. AFSSI 5102, *The Computer Security (COMPUSEC) Program*.

2.1.2.2. AFI 33-104, *Base-Level Planning and Implementation*.

2.1.2.3. AFI 33-112, *Computer Systems Management*.

2.1.2.4. AFI 33-113, *Managing Messaging and Data Processing Centers*.

2.1.2.5. SAF Memo, 31 Jul 98, Foreign National Access to Information Systems.

2.1.2.6. HQ USAF/SCX Message, DTG 110800Z Aug 98, Foreign National Access to the Defense Information System Network (DISN).

2.1.3. Scope. The policies and procedures contained herein cover user access to AFEMS data worldwide.

2.1.4. These procedures cover four access areas: add, change, delete, and reinstate, for both classified and unclassified users of AFEMS. Add, includes initial access; Change, includes access modification; Delete is self-explanatory; Reinstate (via telecon only), occurs when a suspended user is unsuspended.

2.1.5. Add Access. The user obtains forms and instructions from the Local AFEMS Security Administrator (SA) in the Host Chief of Supply (HCOS) access control office or the AFEMS Web site at “<https://www.ilspo.wpafb.af.mil/e-EM/>.” The user completes the form (see attachments 2A1 and 2A2) and returns it to his/her supervisor for review and signature.

NOTE: Foreign national applicants must provide his/her Date of Birth and Home Address in Section IV of the Access Request Form.

2.1.5.1. The user’s supervisor reviews the form for correct information (verifies Top Secret, Secret, or completed Favorable National Agency Check (NAC) for Trustworthiness), signs in the appropriate block and forwards the form to the organization commander.

2.1.5.2. The organization commander (or designated representative) reviews the form for correct information, dates, and signs in the appropriate block, and forwards the form to the local SA in the HCOS access control

office.

2.1.5.3. For Unclassified users, the local HCOS SA reviews the access request for correctness, produces a copy for file and forwards the original to the appropriate major command (MAJCOM) AFEMS point of contact. For Classified users, the local HCOS SA reviews the access request and validates and annotates the security classification information on the request from the Automated Security Clearance Approval System (ASCAS) Roster. If for any reason the security clearance information cannot be verified, the HCOS SA must return the user access request to the user's supervisor for his/her disposition. If all the security information is correct, the HCOS SA will sign the appropriate block, make a copy for file and forward the original to the MAJCOM AFEMS POC.

NOTE: Foreign National AFEMS Access Request Forms only. HCOS SA must have the local Air Force Office of Special Investigation (OSI) obtain a "local records check" and a "government agency records check" for the foreign national applicant. The OSI approval must appear in Section IV of the AFEMS Access Request Form. If the OSI disapproves, the HCOS SA returns the form to the supervisor. If the OSI approves, HCOS SA forwards the Access Request Form to the appropriate MAJCOM AFEMS POC.

2.1.5.4. The MAJCOM AFEMS POC reviews, signs, and forwards the AFEMS Access Request Form to the AFEMS SPO Security Manager.

NOTE: Foreign National Access Request Forms only. MAJCOM commanders are responsible for authorizing foreign national access to information systems within their respective commands. Authorized officials shall not delegate authority below the "three star level" (HQ USAF/CVA ltr, dtd 31 Jul 98, Subj: Foreign National Access to Information Systems). The MAJCOM AFEMS POC will forward the AFEMS Access Request Form package to the appropriate MAJCOM Foreign Disclosure Officer (FDO) for approval. The MAJCOM AFEMS POC forwards the approved package to the AFEMS Security Manager.

2.1.5.5. The AFEMS SPO Security Manager reviews the access request, signs, and forwards the original to the Lockheed Martin CSSO.

2.1.5.6. The CSSO reviews the access request for user access classification level. Both the classified and unclassified users are added, changed, or deleted under the same instructions. Reinstated user accounts are accomplished by telephone only (see paragraph 2.1.8). The only difference is classified users are maintained under a classified account and unclassified users are maintained under an unclassified account.

2.1.5.7. The CSSO creates a user account (User ID and Password), annotates the user Access Request Form and returns it the SPO Security Manager, who forwards the original to the MAJCOM. The MAJCOM returns the original form to the HCOS SA, who annotates the User ID on his/her file copy and forwards the original form to the user with instructions on "Getting Started in AFEMS." All classified user accounts are returned directly to the user.

2.1.6. Change Access.

2.1.6.1. User changes base (PCS) within the same MAJCOM.

2.1.6.2. User changes name resulting from marriage, divorce, etc.

2.1.6.3. User requires changes in data discriminators.

2.1.6.4. Or, user requires organization, office symbol, DSN telephone changes, etc.

NOTE: Follow the procedures in paragraph 2.1.5 for submission of changes.

2.1.7. Delete Access.

2.1.7.1. If the account has been inactive for six (6) months, it will be automatically deleted from the system.

2.1.7.2. Or if the user no longer needs access (retires, new job, PCS, etc.).

2.1.7.3. Supervisor notifies the local HCOS SA that a user access is no longer required.

2.1.7.4. The HCOS SA pulls the file copy of the User Access Request Form, annotates the reason for deleting the access and forwards the copy to the MAJCOM POC. The MAJCOM POC pulls their file copy and annotates the reason for deleting.

2.1.7.5. The MAJCOM forwards the Delete package to the AFEMS SPO Security Manager who pulls the file copy and annotates the reason for deleting the account. The MAJCOM AFEMS POC may elect to complete a systems delete by accessing AFEMS E-mail, Conference, and follow the on-line instructions in “AFEMS – SYSTEM – DELETES.”

2.1.7.6. The CSSO deletes the original User ID, and adds the User ID to the inactive file for audit trail.

2.1.8. Reinstate Access.

2.1.8.1. The user notifies the AFEMS Help desk at DSN 787-4711, option 1, when he/she is locked out of the system, (3 failed attempts unclassified, 2 failed attempts classified). The AFEMS Help Desk resets the User ID and Password.

2.2. User LOGON to AFEMS (C001).

2.2.1. Local LAN accessibility and communication protocol are needed prior to reaching the AFEMS (C001) environment. Local procedures for access should be followed. (See attachment 2A4 for examples of connectivity paths.)

2.2.2. AFEMS initiation screen. This screen contains the system prompt for initiating the AFEMS LOGON sequence. The prompt is located to the right of “ENTER-AWPAFEMS, OR AWPXFER” field, type “AWPAFEMS” then press Enter. This will take the user to the logon screen. (**NOTE:** AWPXFER is for datasets.)

2.2.3. AFEMS LOGON screen. Type in your USERID and PASSWORD (use the tab key to navigate from Userid to Password) and then press the Enter key.

2.2.4. AFEMS informational message display. This screen provides user account information, such as the number of LOGON attempts (count field) and the date and time of last LOGON (last used). Check these values to determine if any unauthorized access attempts have been made. Contact the local security representative if unauthorized access has occurred or suspected. Press the Enter key after checking these values.

2.2.5. AFEMS News Facility. This screen contains information for users from the system administrator. Press the PF8 key to page forward, or press the Enter key to access the AFEMS Main Menu.

2.3. AFEMS Main Menu.

2.3.1. This screen lists several processing options available through AFEMS. To select an option, enter the number of the option at the system prompt or “S” to the left of the option. Multiple options may be selected. Each of the options are explained below as follows: (**NOTE:** Depending on your User Profile the Main Menu and subsequent menu’s may differ in some way. For this chapter’s purpose, we will only list the first six options of the Main Menu that are common to all users.)

2.3.1.1. DATA TRANSACTION option, Classified/Unclassified system. Displays the User Profile Main Menu and provides access to the predefined AFEMS data transaction screens. (A matrix of all screens to user profile is provided in chapter 3, attachment 3A2).

2.3.1.2. EMAIL option, Classified/Unclassified system. E-mail notices are produced for either information or action from C001 processes. Users may send e-mail message to other AFEMS users. Refer to the TRNG screen to access detailed instructions on how to use e-mail; and chapter 3, attachment 3A2 for a matrix of system generated e-mail notices.

2.3.1.3. AD HOC QUERY option, Classified/Unclassified system. Ad Hoc Query is a forms-driven database maintenance and information retrieval tool. Queries are performed on the “query by example” basis. Data is selected by providing user-defined criteria. Common requests may be stored for repeated execution. Output is viewed on-line, or may be downloaded or sent to an authorized printer (refer to paragraph 2.3.1.6 and user screen matrix, chapter 3, attachment 3A2). Refer to AFEMS on-line TRNG screen for detailed instruction on how to use AD HOC QUERY.

2.3.1.4. AD HOC REPORT option, Classified/Unclassified system. Ad Hoc Report is a COTS (Commercial Off-the-Shelf) information retrieval tool that supports query/report writer. Ad Hoc Report uses an “English-like” language to retrieve information from the database. Extensive selection criteria are available to define and select data from one or more C001 database tables. Refer to the AFEMS on-line TRNG screen for detailed instructions on how to use AD HOC REPORT.

2.3.1.5. ON-LINE DOCUMENTS option, Unclassified system only. This COTS product is used for on-line documentation. This product provides the capability for on-line access to various C001 documents, such as Functional Description, Database Specification, and System/subsystem Specification. Refer to the on-line TRNG screen for detailed instructions on On-line Documents.

2.3.1.6. OUTPUT PRODUCTS option, Classified/Unclassified system. Output Products are generated in C001 by users from on-line data transaction screens, Ad Hoc Query /Report, or automatically by the batch scheduler. The user has the option to view output results on-line, print the results on a system recognized printer, create a dataset to transfer the results to a personal computer (PC), save the results for future use, and/or delete the results.

2.3.1.6.1. Print hard copy: All output products may be printed on remote system recognized printers. The application provides a list of all printers available to the user.

2.3.1.6.2. File transfer: All output products may be saved as a dataset for file transfer to the users PC. The PC must have a communication software package with Kermit protocol and sufficient disk storage (floppy/hard disk) available for downloaded data.

2.3.1.6.3. Save: Data put aside for file transfer is stored in a dataset. C001 saves all output products for the following time frames.

2.3.1.6.3.1. Dataset: 48 hours.

2.3.1.6.3.2. Output results: 90 days, except for computed requirements-by-quarter report: 9 months (archive option).

2.3.1.6.4. Refer to on-line TRNG screen for detailed instructions on Output Products.

2.4. Help.

2.4.1. On-line Help Facility (OHF). Explanations to all AFEMS screens and fields are available through the

OHF. Use the PF1 key for screen/field help. Place the cursor in the select field and press PF1. The data displayed will explain how to use the screen. Place the cursor on the field in question and press PF1. The data displayed will explain how to use that field.

2.4.2. AFEMS Functional Guide. For an explanation of how to use OHF and a list of other items of interest to AFEMS users, the AFEMS Functional Guide is available from the AFEMS Main Menu. Select the TRNG screen and press the PF1 key. To print the Functional Guide, press the PF9 key from there.

Attachment 2A1
AFEMS C001 ACCESS REQUEST FORM

SECTION I AFEMS C001 ACCESS REQUEST					
① System access requested: (check only one box)		Classified <input type="checkbox"/> Unclassified <input type="checkbox"/>			
② User request type <input type="checkbox"/> Add <input type="checkbox"/> Delete <input type="checkbox"/> Change Enter ID for delete or change: _____		③ Contract and expiration date <i>AFEMS Program, F33600-90-C-0136, 30 Sep 2001</i>			
④ Last name - first name - middle initial		⑤ Grade / rank	⑥ SSN		
⑦ Position title					
⑧ MAJCOM, organization and station address			⑨ Clearance level		
⑩ Bldg / Post / Room number			⑪ Telephone / DSN Number		
SECTION II					
(a) Check as appropriate	(b) Primary (check only one, enter discriminator if required)	(c) User Profile	(d) ACR Eval	(e) Data Discriminator Information	
				Type	Values
		Air Staff Policy (USAF)			
		MAJCOM (MAJCOM)		MAJCOM(s)	
		AFEMS Policy / System (Policy)			
		Allowance Manager (AM)		AM ID(s)	
		Assessment & Commodity Mgmt (ACM)			
		System Support (SS)		SS ID(s)	
		Item Support (IS)		IS ID(s)	
		Initial Acquisition ORG SPO (SPO)			
		Equipment Management Section (EMS)		SRAN(s)	
		Equipment Custodian (EC)		ORG ID(s)	
② Check the following boxes as appropriate Responsible for correcting errors in the following Data System Designators (DSDs) <input type="checkbox"/> B004 (GLI) <input type="checkbox"/> D002A (SRAN) <input type="checkbox"/> K002 (MAJCOM) <input type="checkbox"/> 0204 (MAJCOM) If additional data discriminators are required, enter below: GLI(s): _____ SRAN(s): _____ MAJCOM(s): _____					
③ <input type="checkbox"/> Responsible for review of C001/PD comparison reports. If additional data discriminators are required, enter below: MAJCOM(s): _____					
④ <input type="checkbox"/> Monitor for ALC Equipment Item Requirements. Circle one of: OC OO SA SM WR					
⑤ I acknowledge my responsibility to: 1. Protect my password at a level commensurate with the highest level of the information on the system 2. Not reveal my password to anyone 3. Not display my password 4. Not give my password to another individual 5. Notify the CSSO and/or my manager of any potential system compromise			⑥ Connectivity path if known (terminal type, ID, etc.)		
⑦ User printed name		Signature	Date		
⑧ Notice: The Privacy Act 5U.C.552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to determine your need and eligibility for access to Government classified information. Although disclosure of your SSN is not mandatory, your failure to do so may result in the denial of your being granted access to classified information associated with your request.					

LOCAL REPRODUCTION IS AUTHORIZED UNTIL AIR FORCE FORM IS PUBLISHED
All Previous Versions Obsolete (Revision C, 21 Jun 94)

SECTION III

Special access requirements

SECTION IV

Remarks and / or disapproval statement

SECTION V

Supervisor name and signature / office symbol

Date _____

DSN

Organization Commander / title / office symbol / signature

Date _____

DSN

Host Chief of Supply / designated representative / signature

Date	
------	--

DSN

MAJCOM Security Officer name and signature

Date

DSN

AFEMS PMO Security Officer name and signature

Date

DSN

SECTION VI (for internal use only)

① Login code / User ID

② Student ID

③ Date access granted

④ DSD system name

⑤ CSSO name and signature

⑥ Date

⑦ DSN

⑧ Password administrator name and signature

⑨ Date

⑩ DSN

Attachment 2A2

INSTRUCTIONS FOR FILLING OUT AFEMS C001 ACCESS REQUEST FORM

SECTION I

<i>BLOCK and TITLE</i>	<i>INSTRUCTION</i>
1 <i>Classified/Unclassified</i>	Check the appropriate block account on either the classified or unclassified AFEMS processor. If user requires access to both, two separate access requests are required. NOTE: Base LAN users are restricted to unclassified access only.
2 <i>User Request Type</i>	Check the appropriate box as to whether this is an add (new account), delete, or a change to an existing account.
3 <i>Contract Number</i>	AFEMS Program, F33600-90-C-0136, 30 Sep 2001.
4 <i>Name</i>	Enter your name.
5 <i>Grade/Rank</i>	Enter your grade/rank.
6 <i>SSN</i>	SSN is required for all access to the classified AFEMS. SSN is optional for access requests to the unclassified AFEMS.
7 <i>Position Title</i>	Self explanatory.
8 <i>MAJCOM, Organization, and Station Address</i>	Enter your three-character MAJCOM code that you're assigned to (see attachment 2A3), your organization office symbol and station address.
9 <i>Clearance Level and date completed</i>	Required only for access requests to the classified AFEMS.
10 <i>Bldg/Post/Room Number</i>	Self-explanatory.
11 <i>Telephone/DSN Number</i>	Self-explanatory.

SECTION II

A *Check as appropriate* Check as many user profiles that apply to your position. At least one user profile must be selected. The following is a list of the User Profiles, what they do, and who can use them:

Air Staff Policy (USAF). Establishes equipment and vehicle management policy. Provides program direction to MAJCOMs via the USAF PD and PMD. Performs readiness assessments and mission simulations. Approves HQ USAF controlled equipment. HQ USAF Surgeon General approves and controls all medical item allowances. Obtains decision management products (e.g., Air Staff users).

MAJCOM (MAJCOM). Evaluates and recommends equipment allowance change request depositions. Reviews and coordinates Support Equipment Recommendation Data (SERD). Implements PD and PMD taskings. Assesses force structure changes. Forecasts time-phased equipment requirements. Maintains reporting organization data. Authorizes command-controlled equipment. Determines asset disposition for excess base funded items. Tracks in-use assets. Identifies War Reserve Materiel (WRM) and vehicle requirements. Performs readiness assessments and simulations. Obtains decision management products (e.g., CEMO (or equivalent), MAJCOM level vehicle managers, and logistics planners).

AFEMS Policy/System (POLICY). Maintains overall surveillance of AFEMS (C001) through continuous review and analysis of allowances, authorizations, and decision management products. Initiates action to add or modify functional requirements to the C001 design. Implements USAF PD and PMD taskings. Assesses impacts of

structure changes. Acts for HQ USAF in the development, approval, disapproval, implementation, and revision equipment allowance standards (AS). Monitors C001 transaction history information and functional statistics. Establishes computation policy and procedures, and maintains surveillance of the computation process (e.g., WR-ALC/LETS, AFEMS SPO staff, and Lockheed Martin staff).

Allowance Manager (AM). Maintains ASs. Coordinates and adjusts equipment allowances based on force structure changes. Reviews and establishes allowances for approved SERDs. Processes allowance change requests. Determines what items are suitable for inclusion in ASs. Conducts weapon system AS reviews with customers. Assesses potential equipment allowances for interchangeability and substitution relationships. Monitors allowance statistics. Obtains decision management products (e.g., Allowance Managers and AFEMS SPO only).

Assessment and Commodity Management (ACM). Assesses overall weapon system supportability and readiness. Implements USAF PD and PMD requirements. Assesses impact of force structure changes. Compiles budget estimates for Program Objective Memorandum (POM) development. Reviews SERDs. Monitors execution of weapon system management plans. Reviews in-use assets and item acquisition status. Obtains decision management products (e.g., System Program Managers (SPM)).

System Support (SS). Assesses weapon system supportability and readiness. Track in-use equipment assets, item acquisition status, allowance change requests, and MAJCOM time-phased equipment requirements forecasts. As directed, contracts for and submits SERDs for evaluation, coordination, approval, and inclusion in ASs. Assesses impacts of force structure changes. Implements USAF PD and PMD taskings. Submits budget estimates POM development. Monitor functional statistics. Obtains decision management products (e.g., SPM).

Item Management (IM) was previously known as Item Support (IS). Controls the buying, stockage, issue, redistribution, and disposition of items. Computes requirements. Determines item substitution and interchangeability relationships. Evaluates equipment allowance change requests and SERDs. Validates requisitions via stock control and distribution functions. Monitors functional statistics, especially items, due-in, IM and ALC statistics. Obtains decision management products (e.g., Inventory Management Specialists (IMS), Equipment Specialists, and Production Management Specialists at the ALCs).

Initial Acquisition Organization (SPO). Contracts for and submits SERDs for evaluation, coordination, approval, and inclusion in ASs. Provides due-in and in-use contract equipment asset information. Implements PMD taskings. Assesses system supportability and readiness. Monitors functional statistics. Obtains decision management products. Submits budget estimates for POM development. Within this profile, acquisition contractors do not have universal read capability of C001. Acquisition contractors are only able to transmit digitized SERDs to C001 and obtain recent confirmation (e.g., SPO).

Equipment Management Element (EME). Evaluates and recommends equipment allowance change request disposition. Establishes equipment authorizations after confirming quantities and basis of issue (BOI) in ASs. Confirms redistribution of assets. Assesses and reports readiness. Implements force structure changes. Monitors transaction history information and functional statistics. Obtains decision management products (e.g., EME, Stock Control, Document Control, REMS Monitors/Managers, Base Vehicle Fleet Managers).

Equipment Custodian (EC). Reviews pertinent ASs. Submits requests for equipment authorization. Originates, coordinates, and monitors equipment allowance change requests. Maintains equipment account records. Confirms organization mission products. Assesses organization mission readiness in support of unit deployments.

B *Primary*

A user with multiple profiles and multiple data discriminators may want to

establish a primary account. The establishment of a primary user account will allow the user to bypass the USER PROFILE and DATA DISCRIMINATOR screen, and proceed directly to the account where the bulk of the work is to be completed. Not establishing a primary user account will result in the display of the USER PROFILE and DATA DISCRIMINATOR screen. Only one account can be selected to be primary. If there are multiple data discriminators associated with the user profile selected to be primary, enter the data discriminator in this column, otherwise just check the appropriate user profile designation.

C *User Profile* There is no action required. This defines the title of the function allowable within AFEMS. This title is used in conjunction with block II A instructions above.

D *ACR Eval* (Allowance Change Request Evaluation). If the user profile selected allows for the designation of and ACR evaluation (AF Form 601 coordinator), and the user is an ACR evaluator, the letter “Y” needs to be entered, e.g., MAJCOM level and above. Leaving this field blank means that the user does not have this authority, e.g., EC.

E *Data Discriminator Information* The user must enter any data discriminators applicable for their tasks. For each user profile, the required data discriminator type identified under the Type column. The data discriminators for each profile is to be entered in the blank line provided. If the space provided is not sufficient for the data discriminators use Section IV (see Section IV comments on the method for annotating the information). Enter the information in accordance with the following guidelines:

- AM ID. Required for the Allowance Manager user profile. The information is the manager ID. The format of the information is to be a three-position alphanumeric code, i.e., ABC, X1B, etc.
- IM ID. Required for the Item Management user profile. The information is the manager ID. The format of this information is to be a three-position alphanumeric code, i.e., ABC, X1B, etc.
- SS ID. Required for the System Support user profile. The information is the System Program Manager ID. The format of this information is to be a three-position alphanumeric code, i.e., ABC, X1B, etc.
- MAJCOM. Required for those users selecting the MAJCOM user profile. Enter the three-position system command code, i.e., AMC for Air Mobility Command. (See attachment 2A3 for valid system command codes.)
- SRAN. Required only for a user assigned to the Equipment Management Element user profile. Enter the six-character code, i.e., FE2300.
- ORG ID. Required only for a user assigned to the Equipment Custodian user profile. Enter the twelve-character organization ID, i.e., 1234TFR50000. **NOTE:** Contact Base Supply if not known.

2 *Check the following boxes as appropriate* Certain users are responsible for correcting errors associated with the various data loads. If you are responsible for correcting data load errors, then you must check the appropriated data system designator box. In parenthesis next to each system is the information required to provide you with specific error correction information through the OUTPUT PRODUCTS options. This additional information needs to be entered as required in the space provided. The SRAN is the six-position alphanumeric, i.e., FE4812. The GLI is the four-position location code, i.e., ABCD. The MAJCOM is the three-position system command code, i.e., MTC. Enter all specific information for which you are responsible.

3 *Responsible for review...* The users responsible for the review and correction of the C001/USAF PD Comparison Reports need to check this box. This report is produced during the load of the PD data and will be provided to the user through the OUTPUT PRODUCTS option. Again, your system command code must be entered. (See attachment 2A3 for valid system command codes.)

4 *Monitor for ALC...* Check if you are the ALC Equipment Requirement Monitor and circle the appropriate ALC. This will provide you with the periodic reports generated through C001 background process, through OUTPUT PRODUCTS. **NOTE:** The POLICY user profiles are provided specific reports based on office symbol. These reports will be established in OUTPUT PRODUCTS on a per user basis. Ensure if you are a policy user profile that your office is provided to Section I.

5 *I acknowledge...* Read the requirements for protecting your user account. If there are any questions contact your security representative.

6 *Connectivity path if known* Describe the communications connectivity path that your terminal will use to reach C001. This information will provide AFEMS Help Desk personnel with information to help resolve any user access problems. If your connectivity path is unknown contact the local communications organization (also see attachment 2A4).

7 *User name, signature, and date* Self-explanatory.

8 *Privacy Act Information* Read for understanding requirements to access classified information.

SECTION III

Enter the special access requirements and a statement to justify the rationale for the access. For example, Security Administrators require access to auditing reports and would state that need.

SECTION IV

Used to provide additional information. In particular, the need to define more user profile/data discriminator combinations than can be clearly documented in Section II. It is recommended that this information be grouped as illustrated in the examples:

MAJCOM/ELM, ICT, AMC

EME/FE2300, FE4826

This will ensure all authorized accounts are accurately established.

Disapproval Statement. Rationale for disapproval of the request. **NOTE:** The individual disapproving the AFEMS C001 Access Request should return the form, through the offices that coordinated on the form to the requester.

SECTION V

Supervisors name... Self-explanatory.

Organization Commander... Or designated representative, self-explanatory, with exceptions for other than base level: ALCs – 4 letter office symbol; MAJCOM HQ – 3 letter office symbol; HQ USAF – 4 letter office symbol.

Host Chief of Supply... Self-explanatory.

MAJCOM ... The MAJCOM AFEMS point of contact (POC).

SECTION VI

This section is completed by the development contractor (Lockheed Martin) and is provided for completeness only.

BLOCK	and TITLE	INSTRUCTION
1	<i>Login code/User ID</i>	Initial login/user ID and password created by the password administrator. (NOTE: The user will log in this user ID and password for initial access. The prompt will tell the user to create a new password.) The initial user ID is maintained in the system and is the only way the user may get the account reset should the user forget the password or be locked out of the system.
2	<i>Student ID</i>	NOT USED ignore this block.
3	<i>Date access granted</i>	Self-explanatory.
4	<i>DSD system name</i>	C001.
5	<i>CSSO name and signature</i>	Development contractor password administrator.
6	<i>Date</i>	Self-explanatory.
7	<i>DSN</i>	Self-explanatory.
8	<i>Password Administrator...</i>	May not be the same as the CSSO.
9	<i>Date</i>	Self-explanatory.
10	<i>DSN</i>	Self-explanatory.

Attachment 2A3**SYSTEM COMMAND CODES****Table 2A1. System Command Codes.**

System Command Code	Command Code	MAJCOM Title (in title sequence)
AAG*	06	AF Audit Agency
BDA	2V	AF Base Disposal Agency
EEC	3W	AF Center for Environmental Excellence
CPC	2C	AF Civilian Personnel Management Center
CBT*	2H	AF Combat Operations Staff
CMC*	0Y	AF Communications Agency
CCE	2A	AF Cost Analysis Agency
AFW	2W	AF District of Washington
ESC	1W	AF Engineering and Services Center

FSA	1Q	AF Flight Standards Agency
FMC	3Y	AF Frequency Management Agency
ISC	02	AF Inspection Center
INT	05	AF Intelligence Agency
LCT	2E	AF Legal Services Center
MEA	01	AF Management Engineering Agency
MPC*	09	AF Manpower and Personnel Center
MFO	4W	AF Medical Logistics Office
MWR	2U	AF Morale, Welfare and Recreation Center
ICT	2G	AF News Center
MSA	2F	AF Office of Medical Support Center
OSP	08	AF Office of Security Police
OSI*	07	AF Office of Special Investigations
TEC	03	AF Operational Test and Evaluation Center
PEO	2R	AF Program Executive
RDF*	3X	AF Rapid Deployment Forces
REA	2X	AF Real Estate Agency
RBO	2M	AF Review Boards Office
SFT	2T	AF Safety Agency
SCB	3J	AF Security Clearance Agency
SOC*	0V	AF Special Operations Command
CSA	2N	AF Studies and Analysis Agency
TAP*	2L	AF Technical Applications Center
ELM	3V	AFELM
ZBD	31	AFELM
EUR	3G	AFELM – Other European Activities
ZLA	3N	AFELM US Atlantic Command
ZEC	3P	AFELM US Central Command
ZPA	3O	AFELM US Pacific Command
ZSA	3M	AFELM US Southern Command
SOE	3D	AFELM US Special Operations Command

SAJ	3Q	AFELM US Strategic Command
MMJ	51	AFMC/XRJ
ACC*	1C	Air Combat Command
AET*	0J	Air Education and Training Command
MTC*	1M	Air Force Materiel Command
AFR*	0M	Air Force Reserve
AMC*	1L	Air Mobility Command
ANG*	4Z	Air National Guard
NGS*	2I	Air National Guard Support Center
RPC*	0I	Air Reserve Personnel Center
AWS	2Q	Air Weather Service
CHF	3L	Center for AF History
DAV	4H	Defense Audiovisual
AFC	0E	Defense Finance and Accounting Service
DMA	88	Defense Mapping Agency
SPC*	1S	HQ Air Force Space Command
ITC*	0U	HQ Air Intelligence Agency
HAF*	0N	HQ USAF
JCS*	41	Joint Communications Support Element
MAP	40	Military Assistance Program Country
PAF*	0R	Pacific Air Forces
RCM	3I	Reserve Central Managed
JMC	8J	San Antonio Joint Military Medical Command
ACD*	0B	US Air Force Academy
AFE*	0D	US Air Forces in Europe
HRS	2K	USAF Historical Research Center

NOTE: “*” denotes the only MAJCOM values that may be used by the SBSS.

Attachment 2A4

CONNECTIVITY PATH

2A4.1. The following diagrams (examples) are common methods to connect terminals to access C001. These

diagrams may not represent all methods to connect to C001. Contact local communications organization for your specific connectivity path.

2A4.2. Abbreviations used in this attachment are:

2A4.2.1. ACN (Automated Commercial Network).

2A4.2.2. APPLID (Application Identifier).

2A4.2.3. DDN (Defense Data Network) (reference only) replaced by NIPRNET.

2A4.2.4. FEP (Front End Processor).

2A4.2.5. LAN (Local Area Network).

2A4.2.6. NCP (Network Control Program).

2A4.2.7. NET (Network).

2A4.2.8. NIPRNET (Nonclassified Internet Protocol Router Network), replaced DDN.

2A4.2.9. PC (Personal Computer).

2A4.2.10. SBLC (Standard Base Level Computer).

2A4.2.11. SNA (System Network Architecture).

2A4.2.12. TAC (Terminal Access Control).

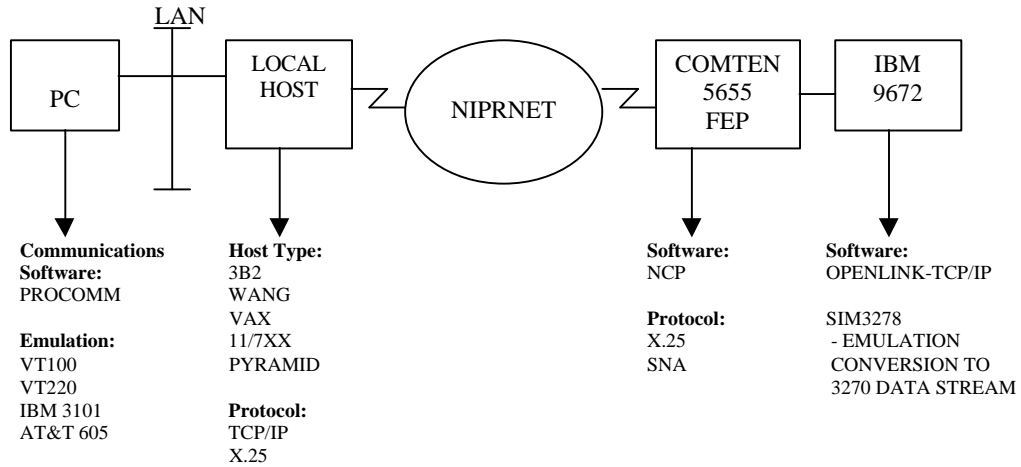
2A4.2.13. TCP/IP (Transmission Control Protocol/Internet Protocol).

2A4.2.14. VTAM (Virtual Telecommunications Access Method).

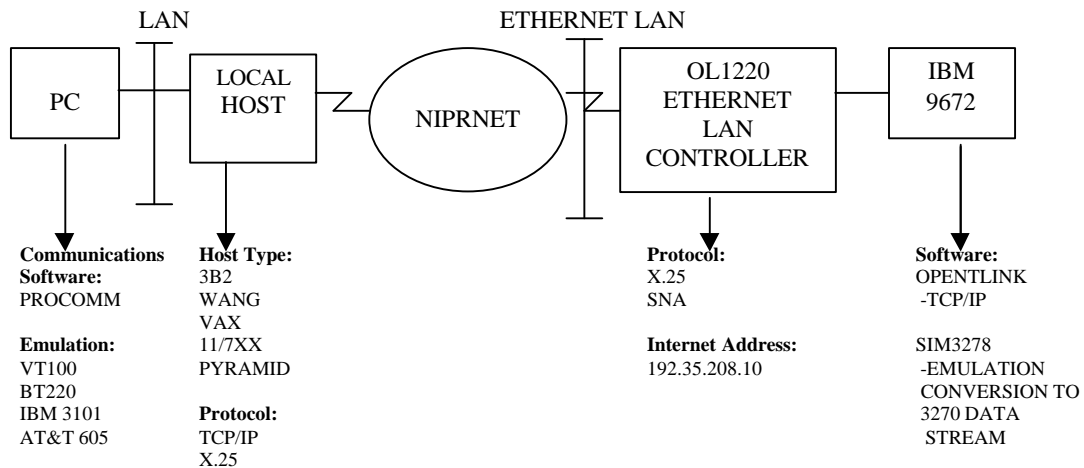
2A4.2.15. W/___ (With).

CONNECTIVITY PATH

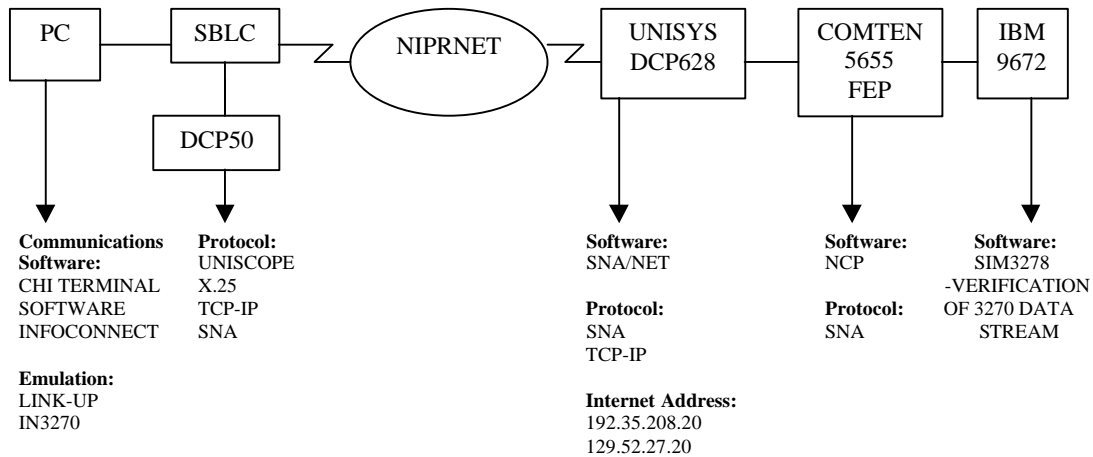
EXAMPLE 1: REMOTE HOST TO COMTEN FEP



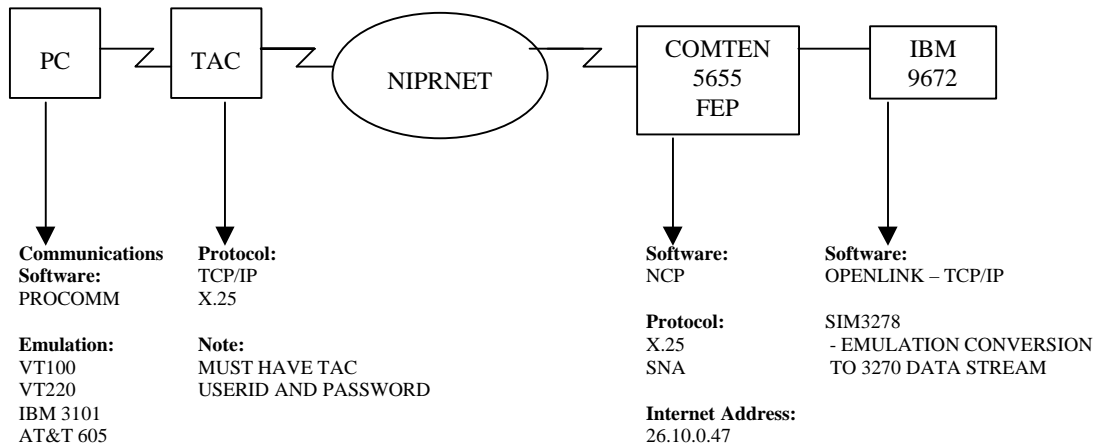
EXAMPLE 2: REMOTE HOST TO ETHERNET LAN CONTROLLER



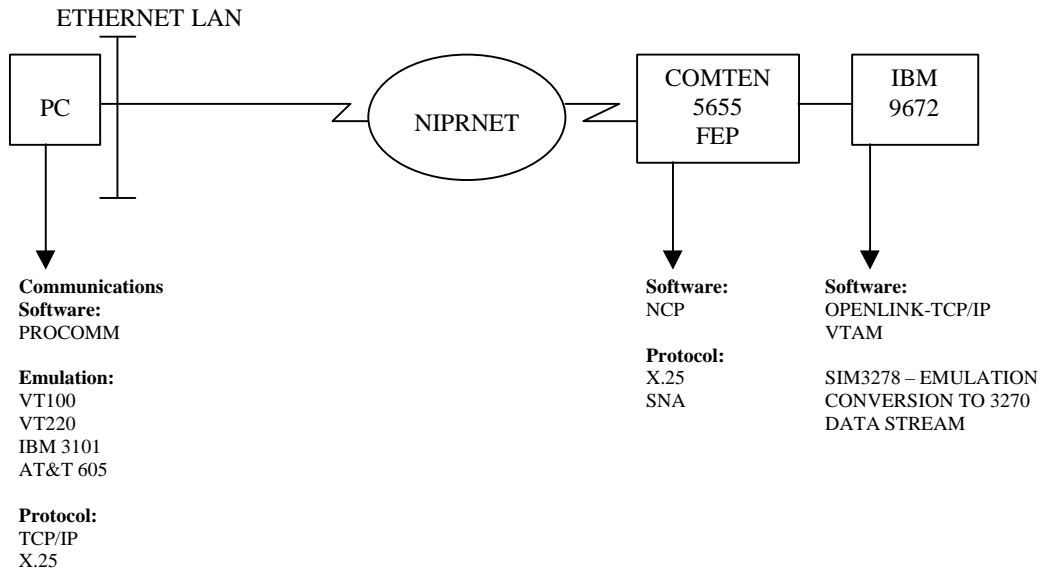
EXAMPLE 3: PC/SBLC TO UNISYS DCP628 FEP



EXAMPLE 4: TERMINAL ACCESS CONTROLLER TO COMTEN



EXAMPLE 5: PC WITH ETHERNET BOARD TO COMTEN



EXAMPLE 6: PC TO SNA GATEWAY

